# EXHIBIT 1-B

DONATE

Elections

# Relying on electronic voting machines puts us at risk, security expert says

How do we make elections secure? Try paper. Professor J. Alex Halderman, a security expert at the University of Michigan, explains why.

Innovation Hub
*August 17, 2020*
By Teresa Lawlor

Maurice Jones prepares to cast mail-in voting ballots for his family on the last day of early voting for the US presidential election at the C. Blythe Andrews, Jr. Public Library in East Tampa, Florida, Aug. 16, 2020.
Octavio Jones/Reuters

In 2018, University of Michigan professor J. Alex Halderman helped conduct a mock election. The question at issue was simple: What is the greatest university, the University of Michigan or Ohio State? (They're rivals.) Predicting the outcome seemed simple because the electorate was composed of University of Michigan students. But the results, generated by electronic voting machines, showed a shocking upset in favor of Ohio State. What happened?

In fact, Halderman had hacked the election before it even began; by installing malicious software on the voting machines, some votes for the University of Michigan were changed as they were cast. Doing so, he says, was "unfortunately, somewhat easier than it sounds." And, according to Halderman, our reliance on electronic voting can make our actual, real-world elections just as vulnerable.

***Related:*** *How the world's largest democracy casts its ballots*

There's been a lot of attention on Russia's efforts to use social media to influence the 2016 election, but their interference didn't end there. Halderman says that Russia probed the electronic election infrastructure of all 50 states and successfully gained access to several voter registration systems. Although subsequent investigations found that they did not manipulate registrations or votes, they may have had the capacity to do so.

***Related:*** *Why Russian interference in elections can be assumed*

"There wasn't anything technological that was stopping them. They didn't change [the registration records] not because the technology put up a barrier but because Vladimir Putin decided not to pull the trigger," says Halderman. "And that's what really worries me. That they could have a lot more damage in 2016, and in many parts of the country, the technology still isn't there to guarantee that they won't be able to do damage in 2020."

But how exactly would it work to hack the vote? Though electronic voting machines may seem disconnected from each other and therefore less susceptible to security threats, the election-specific programming loaded onto each machine comes from the same place.

> "If Russia or other attackers can break into a state's election management system, they can spread malicious software to voting machines throughout that jurisdiction, and potentially change all of the digital records. That's the threat that really keeps me up at night."
> *- J. Alex Halderman, professor, University of Michigan*

"Before every election, every machine has to be programmed with the races, the candidates, the rules for counting. And that programming is made either by the state or local government or an outside vendor on a centralized system called an election management system," Halderman explains. "If Russia or other attackers can break into a state's election management system, they can spread malicious software to voting machines throughout that jurisdiction, and potentially change all of the digital records. That's the threat that really keeps me up at night."

Since 2016, Congress has allocated significant funds to bolster election security. Halderman says that he sees a marked increase in awareness of cybersecurity issues, as well as improvements in cooperation between election officials and law enforcement on this problem. He also reports a decrease in machines that are entirely paperless and therefore the most vulnerable to hacking. Now just 15% of US voters live in areas where voting machines are paperless.

***Related:*** *'COVID-19 is in charge of the census,' says former US Census Bureau director*

But there's a long way to go. Paper ballots are elections' "physical fail-safe" — they're what determines whether or not machines have been compromised. Halderman says that states such as Georgia and South Carolina are now having voters use ballot-marking devices, which use computer inputs to generate paper ballots, rather than limiting that technology to voters with disabilities. A study conducted by Halderman at the University of Michigan last summer found that only 6% of 250 voters noticed that their printed ballot had been altered by a ballot-marking device. Although this set-up is technically paper-based, that crucial fail-safe is gone.

In 2020, an already fragile system is being dramatically reshaped by a pandemic just a few months before the presidential election.

"One of the problems that we're really facing in 2020, is that so much is new and so much is changing, especially due to COVID[-19], that there will almost inevitably be places across the country that experience delays, experience breakdowns, experience long lines or delayed mail-in ballots, and it won't necessarily be due to hacking," says Halderman. Mail-in voting — now available to more Americans than ever before in response to the pandemic — involves a different set of issues; the US Postal Service faces immense challenges, as the Trump-appointed Postmaster General Louis DeJoy displaces top executives and cuts back on overtime, causing mail to pile up.

> "Even if Russia does nothing at all, they'll still be able to point to instances where there were breakdowns, and make it appear that they were due to hacking."
> *- J. Alex Halderman, professor, University of Michigan*

Halderman warns that because of the setbacks and delays that will most likely occur this year, it will be easy for people to claim manipulation or fraud. "Even if Russia does nothing at all, they'll still be able to point to instances where there were breakdowns, and make it appear that they were due to hacking. So, if your goal is just to undermine confidence in the election, in 2020 you probably don't have to do anything at all. And that's because the election system is just not engineered well enough to provide evidence for people that it functioned correctly."

Russia's 2016 election interference called into question the legitimacy of the process. According to Halderman, making sure that we're all doing our part — by carefully checking over our paper ballots, whether we filled them out ourselves or not — is key to getting that legitimacy back.

*Teresa Lawlor is an intern at Innovation Hub. You can follow her on Twitter: @tmlawlor*

## Related Content

Nearly half of Venezuelans are considering leaving the country in the coming months, poll says

Venezuelans are finding creative ways to bypass censorship and a government crackdown on the media

Who are the Venezuelans still backing Nicolás Maduro?

Venezuelans head to the polls on Sunday with many hoping for a change in leadership

Categories:

Tags:

The World

The World is a public radio program that crosses borders and time zones to bring home the stories that matter.

*Produced by:*

PRX

GBH

*Thanks to our sponsor:*

*Major funding provided by:*

About Contact Donate Meet the Team Privacy Terms of use

PRX is a 501(c)(3) organization recognized by the IRS: #263347402.